John P. Mertens
Pia Hoyt Law Firm, LLC
170 South Main, Suite 1100
Salt Lake City, Utah 84101
(801) 350-9000
jmertens@piahoyt.com

Attorney for Plaintiffs

Additional Counsel Included in Signature Block

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

TYLER BAKER and JOSHUA RHOADES, on behalf of themselves and on behalf of all others similarly situated, Plaintiffs, v. HEALTHEQUITY, INC., Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Tyler Baker and Joshua Rhoades, by their undersigned counsel, file this Class Action Complaint individually and on behalf of a class of all similarly situated persons against HealthEquity, Inc. ("Defendant" or "HealthEquity"). Plaintiffs base the following allegations on personal knowledge, due investigation of counsel, and, where indicated, on information and belief, and state in support thereof as follows:

NATURE OF THE ACTION

1. Defendant describes itself as a leader and an innovator in providing technology-enabled services that empower consumers to make healthcare saving and spending decisions. "We use our innovative technology to manage consumers' tax-advantage health savings accounts ("HSA") and other consumer-directed benefits […] offered by employers, including flexible

spending accounts and health reimbursement arrangements […], and to administer [COBRA], commuter and other benefits."[1]

2. As a major provider of healthcare saving and spending services to the United States population, HealthEquity understood it had the duty and responsibility to protect customers' information that it collected, stored, and maintained, expressly advertising to potential customers that its "Remarkable service begins with remarkable trust" and that "[a]s part of our remarkable service, we are committed to protecting the confidentiality, integrity, and availability of your personal information and our systems and applications."[2]

3. HealthEquity further touts its "approach to securing your data against cyber threats" as including "employing secure design and testing practice practices, developing a world-class Security & IT organization, and building strong partnerships across the cybersecurity industry."[3]

4. Contrary to these assurances, however, Defendant failed to meet its duty and, as a direct result, millions of customers' highly sensitive information with which it was entrusted was released and stolen.

5. On July 2, 2024, in a disclosure reported to the Securities and Exchange Commission, Defendant announced that "earlier this year" it became aware of unauthorized access to and disclosure of information including "personally identifiable information, which in some cases is considered protected health information" (the "Data Breach").[4]

---

[1] *2023 Form 10-K for the fiscal year ended January 31, 2024*, HealthEquity (March 22, 2024) https://www.sec.gov/ix?doc=/Archives/edgar/data/0001428336/000142833624000016/hqy-20240131.htm (last accessed August 12, 2024) ("2023 Form 10-K").

[2] *Security & IT*, HealthEquity https://www.healthequity.com/security (last accessed August 12, 2024) ("*Security & IT*").

[3] *Id.*

[4] *Form 8-K*, HealthEquity (July 2, 2024) https://www.sec.gov/ix?doc=/Archives/edgar/data/0001428336/000142833624000055/hqy-20240702.htm (last accessed August 12, 2024) ("Form 8-K")

6. It was not until later that HealthEquity admitted that the personally identifiable information ("PII") and protected health information ("PHI", together with PII, "Protected Information") that was accessed affected *4.3 million* of its customers and included information such as "first name, last name, address, telephone number, employee ID, employer, social security number, health card number, health plan member number, dependent information (for general contact information only), HealthEquity benefit type, diagnoses, prescription details, and payment card information (but not payment card number, and/or HealthEquity account type."[5]

7. In order to utilize Defendant's services, individuals must entrust HealthEquity with sensitive, private information concerning their healthcare, including, upon information and belief, but not limited to, their name, address, telephone number, social security number, health card number, health plan member number, dependent information, diagnoses, prescription details, and payment card information. Defendant requires this information in order to perform its regular business activities and acknowledges that it is highly sensitive.

8. As a direct and proximate result of Defendant's inadequate data security measures and its breach of its duty to handle Protected Information with reasonable care, Plaintiffs' and Class Members' Protected Information have been accessed by hackers and exposed to an untold number of unauthorized individuals.

9. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their privacy, and similar forms of criminal mischief, which may last for the rest of their lives.

[5] *Notice of Data Breach*, HealthEquity, https://www.healthequity.com/breach (last accessed August 12, 2024) ("*Notice of Data Breach*"); Zack Whittaker, *HealthEquity data breach affects 4.3M people*, Tech Crunch (July 30, 2024), https://techcrunch.com/2024/07/30/healthequity-data-breach-affects-4-3-million-people/ (last accessed August 12, 2024).

Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. Plaintiffs, on behalf of themselves, and the Class, as defined herein, bring claims for negligence, negligence *per se*, breach of an implied contract, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

12. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District and maintains its principal place of business in this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

PARTIES

14. Plaintiff Tyler Baker is an adult who, at all relevant times, is and was a citizen and resident of the State of Vermont. Plaintiff used HealthEquity from March of 2021 through March 2023 to coordinate payments of his daycare premiums.

15. Plaintiff Joshua Rhoades is an adult who, at all relevant times, is and was a citizen and resident of the State of Pennsylvania. Plaintiff used HealthEquity since 2020 to coordinate payments for appointments with his primary care doctor, specialists, and physiotherapists.

16. Since the unauthorized access of information in the Data Breach, Plaintiffs have received a significant increase in spam calls compared to prior to the Data Breach and have suffered emotional distress as a result of their Protected Information being accessed and exposed to unauthorized third parties.

17. As a result of the Data Breach, Plaintiffs will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

18. HealthEquity, Inc. is a corporation organized under the laws of Delaware and maintains its headquarters and principal place of business in Draper, Utah.

FACTUAL BACKGROUND

A. Defendant Collected Plaintiffs' and Class Members' Protected Information as a Necessary Part of Its Routine Business Dealings with Them.

19. HealthEquity describes its core offerings as the HSA, a financial account through which its customers spend and save long-term for healthcare expenses on a tax-advantaged basis. As of January 31, 2024, HealthEquity administered 8.7 million HSAs, with balances totaling $25.2 billion, as well as 7 million complementary customer-directed benefits. HealthEquity is the largest HSA provider and the largest provider of customer-directed benefits.[6]

20. As a condition of receiving HealthEquity's services, its customers must provide it with sensitive Protected Information, which includes, upon information and belief, full name, address, telephone number, social security number, health card number, health plan member number, dependent information, diagnoses, prescription details, and payment card information.

[6] *2023 Form 10-K.*

21. HealthEquity derives substantial benefit from this information because, but for the collection of Plaintiffs' and Class Members' Protected Information, Defendant would be unable to perform its various services.

22. Defendant acknowledges that the information it collects is highly sensitive and triggers heightened protections. For example, Defendant concedes that "[b]ecause we perform services (such as FSA services) for covered entities that include processing protected health information, we are a business associate and subject to [the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")]. The two rules that most significantly affect our business are […] the Privacy Rule […] and (ii) the Security Standards for the Protection of Electronic Protected Health Information, or the Security Rule. […] The Security Rule establishes requirements for safeguarding protected health information transmitted or stored electronically. Both civil and criminal penalties apply for violating HIPAA, which may be enforced by both the Department of Health and Human Services' Office for Civil Rights and state attorneys general. Violations of HIPAA may also subject us to contractual remedies under the terms of business associate agreements with covered entities."[7]

23. Accordingly, HealthEquity acknowledges the vast amounts of Protected Information with which it is entrusted, claiming that "as part of our remarkable service, we are committed to protecting the privacy of your personal information" and "[w]e believe protecting data is a fundamental component of connecting health and wealth." Defendant advertises its use of "up to date administrative, physical, and technical safeguards to protect personal information"

[7] *2023 Form 10-K.*

and claims its "team members and business partners are trained on and accountable for complying with our privacy policies and standards."[8]

24. HealthEquity also openly boasts of its cybersecurity practices, claiming to "follow a defense-in-depth security model with a Joint Security Operations Center (JSOC) and Data Protection team working with security architects and engineers deploying controls designed to prevent or limit the success of an attack" that leverage "the best practices of fraud prevention and cybersecurity monitoring to protect the transactions of our members and clients." "We are committed to protecting the confidentiality, integrity, and availability of your personal information and our systems and applications." Defendant also displays a "HIPAA Compliance" badge.[9]

25. Plaintiffs and Class Members directly or indirectly entrusted HealthEquity with their sensitive and confidential Protected Information and therefore reasonably expected that Defendant would safeguard it and keep it confidential.

26. By obtaining, collecting, and storing Plaintiffs' and Class Members' Protected Information, HealthEquity assumed equitable and legal duties to safeguard and keep confidential Plaintiffs' and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

27. Despite these duties, HealthEquity failed to implement reasonable data security measures to protect Plaintiffs' and Class Members' Protected Information and ultimately allowed nefarious third-party hackers to breach its computer systems, compromising Plaintiffs' and Class Members' Protected Information stored therein.

B. HealthEquity Knew the Risks of Storing Valuable Protected Information and the Foreseeable Risk of Harm to Victims.

[8] *Privacy*, HealthEquity, https://www.healthequity.com/privacy (last accessed August 12, 2024).
[9] *Security & IT*

28. HealthEquity was well aware that the Protected Information it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

29. HealthEquity also knew that a breach of its computer systems, and release of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Protected Information was compromised, as well as intrusion into their highly private information.

30. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem, AT&T, and many others.

31. Protected Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft and medical and financial fraud.[10] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Protected Information on multiple underground Internet websites, commonly referred to as the "dark web."

32. Criminals often trade stolen Protected Information on the "cyber black market" for years following a breach. Cybercriminals can also post stolen Protected Information on the internet, thereby making such information publicly available. Indeed, the information compromised during the Data Breach may already have been released on the internet.

33. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2023, there were 3,205 data compromises affecting 353

[10] *What To Know About Identity Theft*, Fed. Trade Comm'n Consumer Advice (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed August 12, 2024).

million individuals, which set a record high number of data compromises in the U.S. in a single year, representing a 72% increase from the previous all-time high number of comprises set in 2021.[11]

34. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2019, approximately 650,000 people reported identity fraud compared to over a million people in 2023, representing an increase of approximately 19%.[12]

35. The breadth of data compromised makes the information particularly vulnerable to thieves and leaves HealthEquity's customers especially vulnerable to fraud and other risks.

36. The ramifications of HealthEquity's failure to keep Plaintiffs' and Class Members' Protected Information secure are long-lasting and severe. Once Protected Information is stolen, fraudulent use of that information and damage to victims may continue for years.

37. Further, a data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[13]

---

[11] *Facts + Statistics; Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last accessed August 12, 2024).

[12] *Id*.

[13] Erika Harrell, Bureau of Just. Stat., U.S. Dep't of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed August 12, 2024).

38. Even if stolen Protected Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained Protected Information about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

39. Moreover, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, information such as social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies to update the person's accounts with those entities.

40. The Social Security Administration even warns that the process of replacing a social security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[14]

41. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of Protected Information to steal and then sell.

42. Moreover, healthcare information is a particularly attractive target in data breaches. Whereas cybercriminals may be able to sell credit card information for $20, patients' medical records can go for $60 or $70, and complete identity theft kits including health insurance credentials may be worth up to $1,000 on the black market.[15] Keeping healthcare information secure is an equally important priority to Plaintiffs and Class Members. For example, Experian notes that, while identity theft victims often have to spend $600 in response to problems related to having their data stolen, healthcare identity theft victims spend nearly $13,500 dealing with their

---

[14] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed August 12, 2024).

[15] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), IDExperts, https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last accessed August 12, 2024); *Managing cyber risks in an interconnected world*, PWC, (September 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last accessed August 12, 2024).

hassles, which can include the cost of paying off fraudulent medical bills.[16] Victims of healthcare data breaches may also be denied care, coverage, or reimbursement by medical insurers, have their policies cancelled, or have to pay to reinstate insurance.

43. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[17]

44. In light of high-profile data breaches at other companies, HealthEquity knew or should have known that its computer systems would be targeted by cybercriminals.

45. Defendant also knew or should have known the importance of safeguarding the Protected Information with which it was entrusted and of the foreseeable consequences if its data security systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach and release of its customers' Protected Information from occurring.

C. Defendant Released Highly Sensitive Protected Information to Hackers and Breached its Duty to Protect Customer Protected Information.

46. According to the notice posted on Defendant's website ("Notice") regarding the Data Breach,[18] HealthEquity was alerted on March 25, 2024 of a system anomaly leading to HealthEquity's determination on June 26, 2024 that its customer's Protected Information was unlawfully accessed.

---

[16] *Health Care Data Breach: What to Know About Them and What to Do After One*, Experian (March 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed August 12, 2024).
[17] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed August 12, 2024).
[18] *Notice of Data Breach*.

47. Defendant's Notice advised, in part, that leaked information pertaining to its customers included one or more of the following categories: first name, last name, address, telephone number, employee ID, employer, social security number, health card number, health plan member number, dependent information (for general contact information only), HealthEquity benefit type, diagnoses, prescription details, and payment card information (but not payment card number), and / or HealthEquity account type.

48. The Notice did not disclose when the unauthorized intrusion occurred or how many customers' information was impacted. However, Defendant separately reported that the Data Breach affected the records of 4.3 million individuals.[19]

49. In sum, upon information and belief, as a result of Defendant's failure to implement adequate data security measures, Plaintiffs' and Class Members' Protected Information was negligently released to unauthorized, malicious threat actors and is now at risk of further dissemination and use by other unauthorized individuals or cybercrime groups.

D. Defendant Failed to Comply with FTC Guidelines.

50. HealthEquity is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

[19] *Data Breach Notifications*, Office of the Maine Attorney General, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed August 12, 2024).

51. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

52. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures, including:[21]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

[20] *Start with Security: A Guide for Business*, Fed. Trade Comm'n (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed August 12, 2024).

[21] *Protecting Personal Information: A Guide for Business*, U.S. FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed August 12, 2024).

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

54. Upon information and belief, HealthEquity failed to properly implement one or more of the basic data security practices described above. HealthEquity's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer Protected Information resulted in the unauthorized release of Plaintiffs' and Class Members' Protected Information to a nefarious threat actor. Further, HealthEquity's failure to implement basic data security practices constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

55. HealthEquity was at all times fully aware of its obligations to protect the Protected Information of consumers because of its business model of collecting Protected Information and storing payment information. HealthEquity was also aware of the significant repercussions that would result from its failure to do so.

56. HealthEquity's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiffs and Members of the Class Have Suffered Concrete Injury.

57. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs, and members of the Class, significant injuries and harm in several ways. Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

58. Once Protected Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason,

Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendant's conduct. Further, the value of Plaintiffs' and Class Members' Protected Information has been diminished by their exposure in the Data Breach.

59. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Protected Information.

60. In 2021 alone, identity theft victims in the United States had financial losses totaling $16.4 billion.[22]

61. Besides the monetary damage sustained, consumers may also spend anywhere from one day to more than six months resolving identity theft issues.[23]

62. Ultimately, the time that victims spend monitoring and resolving identity theft issues takes an emotional toll. Approximately 80% of victims of identity theft experienced some type of emotional distress, and more than one-third of victims experienced moderate or severe emotional distress.[24]

63. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Protected Information.

64. As a result of HealthEquity's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their highly valuable Protected Information; the imminent and certainly impending injury

[22] Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, U.S. Dept. Just., Bureau Just. Stats. (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf (last accessed August 12, 2024).
[23] *Id.*
[24] *Id.*

flowing from fraud and identity theft posed by their Protected Information being placed in the hands of criminals; damages to and diminution in value of their Protected Information that was entrusted to Defendant with the understanding the Defendant would safeguard the Protected Information against disclosure; and continued risk to Plaintiffs' and the Class Members' Protected Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Protected Information with which it was entrusted.

F. Plaintiffs and Members of the Class Are Now at an Increased Risk of Future Harms.

65. Data Breaches such as the one experienced by Plaintiffs and Class Members are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

66. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[25] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiffs and Class Members) must take after a Data Breach like HealthEquity's are both time-consuming and of only limited and short-term effectiveness.

67. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

---

[25] Government Accountability Off., "Data Breaches" (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last accessed August 12, 2024).

[26] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," Government Accountability Off. (June 2007), https://www.gao.gov/new.items/d07737.pdf ("2007 GAO Report") (last accessed April 4, 2024).

68. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

69. Theft of Protected Information is also gravely serious as Protected Information is a valuable property right.[28]

70. There may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Protected Information is stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

71. Protected Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

72. Because the entirety of the stolen information has *already* been released on the dark web, every Class Member, including Plaintiff, is at an increased risk of fraud and identity theft for

---

[27] *See* Identity Theft Victim Checklist, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last accessed August 12, 2024).

[28] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("SPI") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("SPI, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[29] *See* 2007 GAO Report, at 29.

many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

G. Plaintiff Tyler Baker's Experience.

73. Plaintiff Baker has used HealthEquity from March of 2021 through March 2023 to coordinate payments of his daycare premiums. In order to use HealthEquity's services, Plaintiff Baker was required to provide his Protected Information to HealthEquity in exchange for the provision of its services, including, *inter alia*: his name, address, telephone number, social security number, health card number, health plan member number, dependent information, diagnoses, prescription details, and payment card information. When providing Defendant with his Protected Information, Plaintiff expected that his Protected Information would be kept confidential.

74. At all relevant times, Plaintiff has been very careful in sharing and storing his Protected Information. He stores documents containing this information in a safe location and has not knowingly transmitted such information in an unencrypted or unsecure fashion.

75. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Baker's Protected Information in its systems, which Protected Information was improperly accessed and obtained by unauthorized individuals in the Data Breach. Plaintiff Baker did not consent to Defendant's release of his Protected Information to threat actors.

76. Since the Data Breach, Plaintiff Baker has spent numerous hours taking action to mitigate the impact of the Data Breach, which included additional review and monitoring of his personal and financial accounts, endeavoring to implement additional security measures where appropriate, researching credit card monitoring services, and obtaining and making payments for said credit monitoring services. Plaintiff Baker took these mitigation efforts and incurred this loss of time as a direct and proximate result of the Data Breach.

77. Knowing that a threat actor stole his Protected Information and that it may be publicly available on the internet has caused Plaintiff Baker significant anxiety. He is now very concerned about identity theft and impending privacy harms arising from the Data Breach. Plaintiff Baker further has concerns of Defendant suffering future data breaches or otherwise releasing Plaintiff Baker's Protected Information in the future.

78. Plaintiff Baker has suffered actual injury from having his Protected Information exposed as a result of the Data Breach, including, but not limited to: (a) providing his Protected Information to HealthEquity in exchange for its services that Plaintiff Baker would not have paid for had it disclosed that it lacked data security practices to safeguard its customers' Protected Information from theft; (b) damages to and diminution in value of his Protected Information—a form of intangible property that Plaintiff Baker entrusted to HealthEquity; (c) loss of privacy; (d) lost time; and (e) imminent and impending injury arising from the increased risk of fraud and identity theft.

79. As a result of the Data Breach, Plaintiff Baker will continue to be at a heightened risk for identity theft and attendant damages for years to come.

H. Plaintiff Joshua Rhoades' Experience.

80. Plaintiff Rhoades has used HealthEquity since 2020 to coordinate his payments for appointments with his primary care doctor, specialists, and physiotherapists. In order to use HealthEquity's services, Plaintiff Rhoades was required to provide his Protected Information to HealthEquity in exchange for the provision of its services, including, *inter alia*: his name, address, telephone number, social security number, health card number, health plan member number, dependent information, diagnoses, prescription details, and payment card information. When providing Defendant with his Protected Information, Plaintiff expected that his Protected Information would be kept confidential.

81. At all relevant times, Plaintiff has been very careful in sharing and storing his Protected Information. He stores documents containing this information in a safe location and has not knowingly transmitted such information in an unencrypted or unsecure fashion.

82. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Rhoades' Protected Information in its systems, which Protected Information was improperly accessed and obtained by unauthorized individuals in the Data Breach. Plaintiff Rhoades did not consent to Defendant's release of his Protected Information to threat actors.

83. Since the Data Breach, Plaintiff Rhoades has spent numerous hours taking action to mitigate the impact of the Data Breach, which included additional review and monitoring of his personal and financial accounts, endeavoring to implement additional security measures where appropriate, researching credit card monitoring services, and obtaining and making payments for said credit monitoring services. Plaintiff Rhoades took these mitigation efforts and incurred this loss of time as a direct and proximate result of the Data Breach.

84. Knowing that a threat actor stole his Protected Information and that it may be publicly available on the internet has caused Plaintiff Rhoades significant anxiety. He is now very concerned about identity theft and impending privacy harms arising from the Data Breach. Plaintiff Rhoades further has concerns of Defendant suffering future data breaches or otherwise releasing Plaintiff Rhoades' Protected Information in the future.

85. Plaintiff Rhoades has suffered actual injury from having his Protected information exposed as a result of the Data Breach, including, but not limited to: (a) providing his Protected Information to HealthEquity in exchange for its services that Plaintiff Rhoades would not have paid for had it disclosed that it lacked data security practices to safeguard its customers' Protected Information from theft; (b) damages to and diminution in value of his Protected Information—a

form of intangible property that Plaintiff Rhoades entrusted to HealthEquity; (c) loss of privacy; (d) lost time; and (e) imminent and impending injury arising from the increased risk of fraud and identity theft.

86. As a result of the Data Breach, Plaintiff Rhoades will continue to be at a heightened risk for identity theft and attendant damages for years to come.

CLASS ALLEGATIONS

87. Plaintiffs brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose Protected Information was compromised in the HealthEquity Data Breach.

88. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

89. Plaintiffs reserve the right to modify or amend the definition of the proposed Class prior to moving for class certification.

90. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. The number of individuals implicated in the Data Breach is reported to be 4.3 million.

91. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the Protected Information of Plaintiffs and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' Protected Information, and breached its duties thereby;

c. Whether Defendant obtained Plaintiffs' and Class Members' Protected Information;

d. Whether Defendant released Plaintiffs' and Class members' Protected Information without authorization;

e. When Defendant learned of the Data Breach;

f. Whether Defendant adequately and timely responded to the Data Breach;

g. Whether Defendant failed to maintain reasonable security systems and procedures, including those required by applicable security laws and regulations and those consistent with industry standards;

h. Whether Defendant remedied the vulnerabilities that permitted the Data Breach to occur;

i. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or other equitable relief as a result of Defendant's wrongful conduct; and

j. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

92. **Typicality.** Plaintiffs' claims are typical of the claims of the Class Members. The claims of Plaintiffs and Class Members are based on the same legal theories and arise from the

same failure by Defendant to safeguard their Protected Information. Plaintiffs and Class Members entrusted Defendant with their Protected Information, and it was subsequently released to an unauthorized third party and may be publicly available on the internet.

93. **Adequacy of Representation.** Plaintiffs are an adequate representative of the Class because their interests do not conflict with the interests of the other Class Members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation and data breach litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

94. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

95. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the

Class. If Defendant breached its duty and released Plaintiffs' and Class Members' Protected Information, then Plaintiffs and each Class member suffered damages by that conduct.

96. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On behalf of Plaintiffs and the Class)

97. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

98. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Protected Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

99. HealthEquity's duty to use reasonable care arose from several sources, including but not limited to those described below.

100. Defendant has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By receiving, maintaining, and handling Protected Information that is routinely targeted by criminals for unauthorized access, HealthEquity was obligated to act with reasonable care to protect against these foreseeable threats.

101. HealthEquity breached the duties owed to Plaintiffs and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiffs at this time, on information and belief, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to

occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Protected Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive Protected Information.

102. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' Protected Information would not have been compromised.

103. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Protected Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts; and dealing with an increase in spam communications;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Protected Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Protected Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Protected Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of Protected Information to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

104. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(Plaintiffs on Behalf of the Class)

105. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

106. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect Protected Information. Various FTC publications and orders also form the basis of HealthEquity's duty.

107. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Protected Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Protected Information it obtained and stored and the foreseeable consequences of a data breach involving the Protected Information it entrusted from its customers.

108. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

109. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

110. Defendant also violated HIPAA's Security Rule, which requires it to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect

against any reasonably anticipated uses or disclosures of such information that are not permitted; and ensure compliance by its workforce. 45 C.F.R. § 164.306.

111. HIPAA also requires HealthEquity to: "review and modify the security measures implemented […] as needed to continue provision of reasonable and appropriate protection to electronic protected health information" (45 C.F.R. § 164.306(e); "[i]mplement technical policies and procedure for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights" (45 C.F.R. § 164.312(a)(1)); and provide notice of the Data Breach "without unreasonable delay and in no case later than 60 days following discovery of the breach" (45 C.F. R. §§ 164.400-414).

112. Defendant's violation of HIPAA also constitutes negligence *per se*.

113. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act and HIPAA are intended to guard against.

114. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Protected Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts; and dealing with an increase in spam communications;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Protected Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Protected Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Protected Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of Protected Information to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

115. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiffs on Behalf of the Class)

116. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

117. Plaintiffs bring this claim individually and on behalf of the Class.

118. When Plaintiffs and members of the Class provided their Protected Information to Defendant in exchange for their services, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiffs' and Class Members' Protected Information, comply with their statutory and common law duties to protect Plaintiffs' and Class Members' Protected Information, and to timely notify them in the event of a data breach.

119. Defendant solicited and invited Plaintiffs and Class Members, directly or indirectly, to provide their Protected Information as part of Defendant's provision of healthcare administration services. Plaintiffs and Class Members accepted Defendant's offers when they utilized Defendant's services and provided their Protected Information to Defendant.

120. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with their statutory and common law duties to adequately protect Plaintiffs' and Class Members' Protected Information and to timely notify them in the event of a data breach.

121. Defendant's implied promise to safeguard customer Protected Information is evidenced by, *e.g.*, the representations in Defendant's privacy notice and other statements made by Defendant concerning its cybersecurity measures, as set forth in part *supra*.

122. Plaintiffs and Class Members conferred a monetary benefit to Defendant by using its services and making payments through its platform. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of that benefit, and part of the funds Defendant earned through Plaintiffs' and Class Members' use of its services, to obtain adequate data security. Defendant failed to do so.

123. Plaintiffs and Class Members would not have provided their Protected Information to Defendant had they known that Defendant would not safeguard their Protected Information, as promised.

124. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

125. Defendant breached its implied contract with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' Protected Information.

126. The losses and damages Plaintiffs and Class Members sustained, include, but are not limited to:

a. Theft of their Protected Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts; and dealing with an increase in spam communications;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Protected Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Protected Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Protected Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of Protected Information to strangers likely to have criminal intentions and now have

prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

127. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiffs on Behalf of the Class)

128. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

129. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to Plaintiffs' Breach of Implied Contract claim.

130. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

131. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known only to Defendant.

132. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they utilized Defendant's administration services to administer healthcare payments and in so doing provided Defendant with their Protected Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and have their Protected Information protected with adequate data security.

133. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Protected Information of Plaintiffs and Class Members for business purposes.

134. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Protected Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

135. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

136. Defendant failed to secure Plaintiffs' and Class Members' Protected Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

137. Defendant acquired the Protected Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

138. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Protected Information, they would not have agreed to provide their Protected Information to Defendant.

139. Plaintiffs and Class Members have no adequate remedy at law.

140. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have sustained injuries, including, but not limited to:

a. Theft of their Protected Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts; and dealing with an increase in spam communications;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Protected Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Protected Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Protected Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of Protected Information to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

141. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered damages and will continue to suffer other forms of injury and/or harm.

142. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiffs on Behalf of the Class)

143. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

144. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

145. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Protected Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Protected Information. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Protected Information and remains at imminent risk that further compromises of their Protected Information will occur in the future.

146. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed a legal duty to secure customers' Protected Information under the common law and Section 5 of the FTC Act; and

b. Defendant breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Protected Information.

147. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect customers' Protected Information.

148. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at HealthEquity. The risk of another such breach is real, immediate, and substantial. If another breach at HealthEquity occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

149. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

150. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at HealthEquity, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and customers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: August 13, 2024

Respectfully submitted,

/s/ John P. Mertens

John P. Mertens
Pia Hoyt Law Firm, LLC
170 South Main, Suite 1100
Salt Lake City, Utah 84101
(801) 350-9000
jmertens@piahoyt.com

Jonathan M. Jagher*
FREED KANNER LONDON & MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
610.234.6486
jjagher@fklmlaw.com

Douglas A. Millen*
Nicholas R. Lange*
FREED KANNER LONDON & MILLEN LLC
100 Tri-State International Drive, Suite 128
Lincolnshire, IL 60629
224.632.4500
nlange@fklmlaw.com
dmillen@fklmlaw.com

William E. Hoese*
Zahra R. Dean*
Elias Kohn*
Kohn Swift & Graf, P.C.
1600 Market Street, Suite 2500
Philadelphia, PA 19103
(215) 238-1700
whoese@kohnswift.com
zdean@kohnswift.com
ekohn@kohnswift.com

**pro hac vice forthcoming*